WAVESTONE

How mature are annual reports of the CAC 40 regarding cybersecurity?

June 2018

Gérôme BILLOIS
Partner
gerome.billois@wavestone.com
+33 (0)6 10 99 00 60
@gbillois

Alexandre LUKAT
Senior Consultant
alexandre.lukat@wavestone.com
+33 (0)6 72 58 26 52

In a world where permanent evolution is the key to success, Wavestone's mission is to enlighten and partner with business leaders in their most critical decisions.

Tier one clients
leaders in their industry

2,800 professionals
across 8 countries

Among the leading independent consultancies in Europe,
n°1 in France

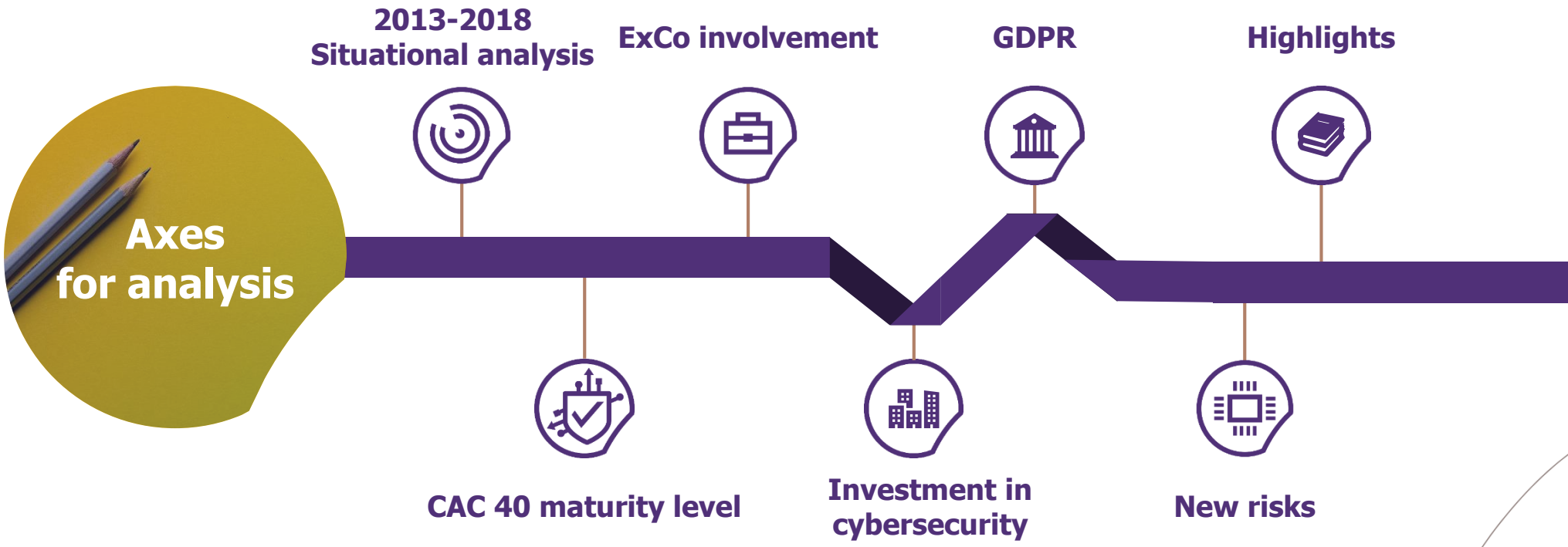
Paris | London | New York | Hong Kong | Singapore* | Dubai* | São Paulo*
Luxembourg | Madrid* | Milano* | Brussels | Geneva | Casablanca | Istanbul* | Edinburgh
Lyon | Marseille | Nantes

* Partners

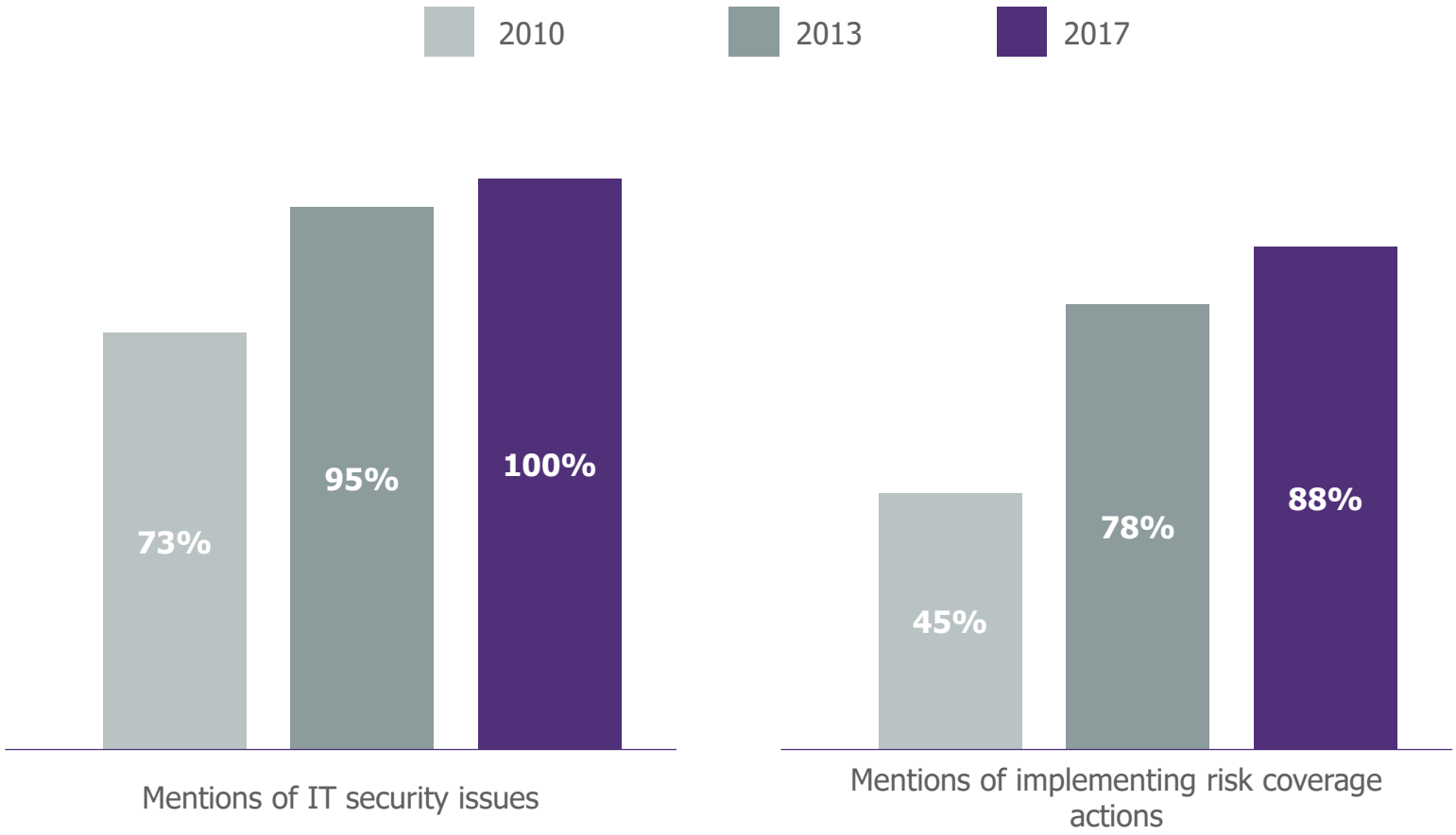
How mature is the CAC 40 in cybersecurity?

Method: this study is based upon a factual analysis of the most recent annual reports and reference documents, published by the CAC 40 companies on 01/06/2018.

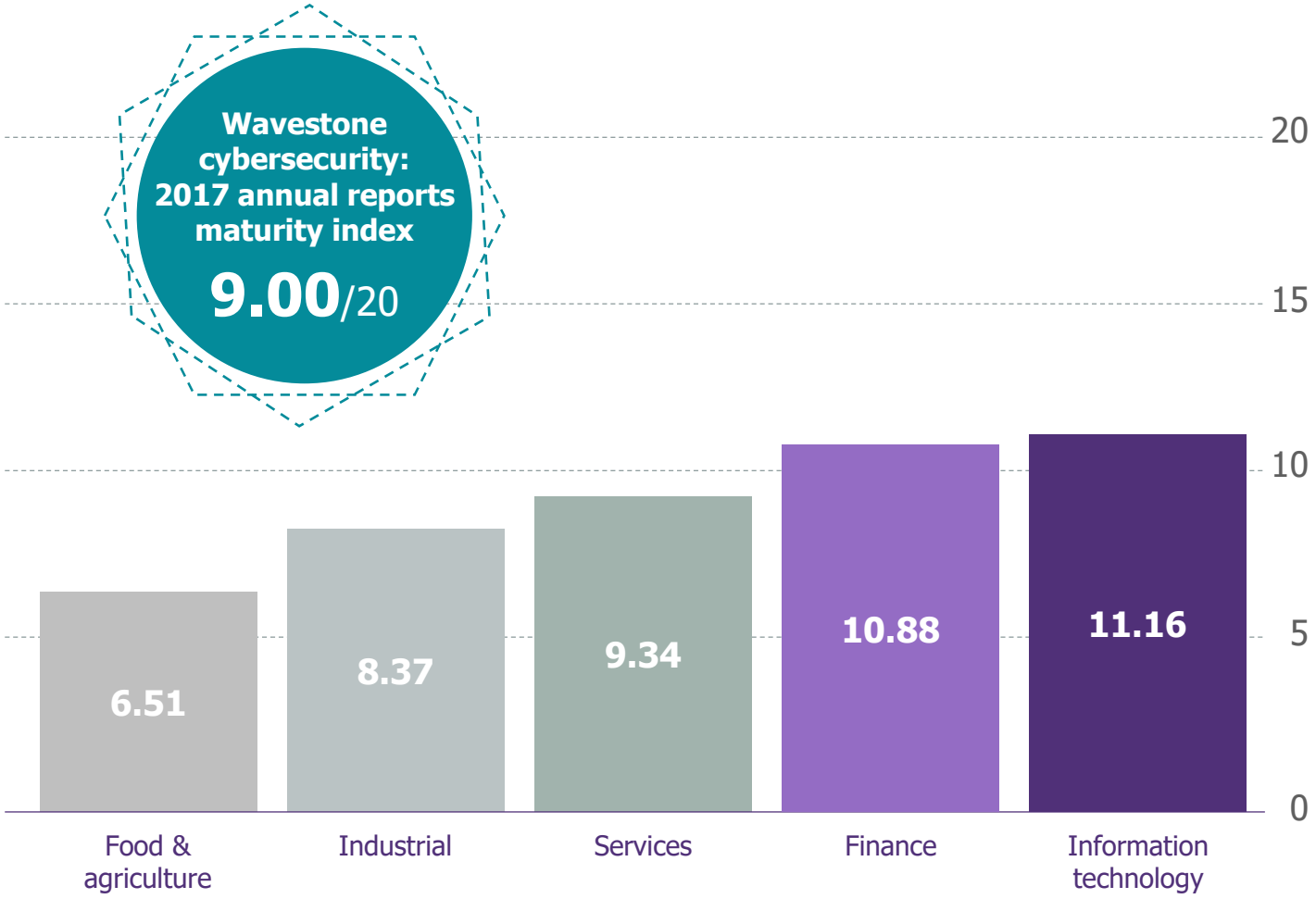
This analysis is based solely on the elements set out within these documents. It should be noted that they do not always reflect the completeness of actions underway in the field.



Finally 100% of CAC 40 companies are acting on cybersecurity



Finance and Information technology sectors stand out



Wavestone cybersecurity: 2017 annual reports maturity index

The *Wavestone cybersecurity: annual reports maturity index* provides an assessment of companies' maturity levels, based upon the content of their reference document. This index, scored out of 20, is based on 14 criteria weighted and marked between 0 and 2. These criteria* cover the following topics:

Issues and risks
Infosec issues, cyber risks and impacts, cyber insurance coverage, digital transformation and new technology security.

Governance and regulation
Executive Committee involvement, ISS governance, personal data protection, awareness and training, transparency vis-à-vis security incidents, regulations and respecting standards.

Protection and Controls
Action plan implementation, cybersecurity programme, securing business systems, audits and controls.

**The full assessment criteria are set out in the appendix*

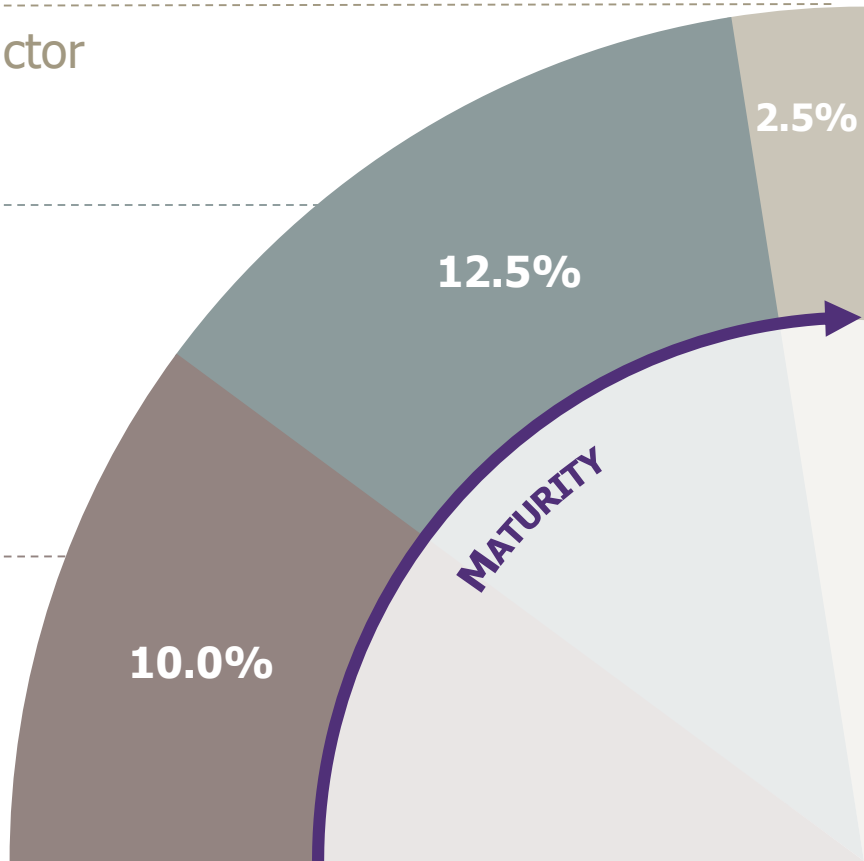
Executive committees ever more involved

25% of CAC 40 groups address the question of cybersecurity at executive committee level.

A member of the executive committee is an active actor in cybersecurity.

A governance body addresses cybersecurity with the executive committee on a regular basis.

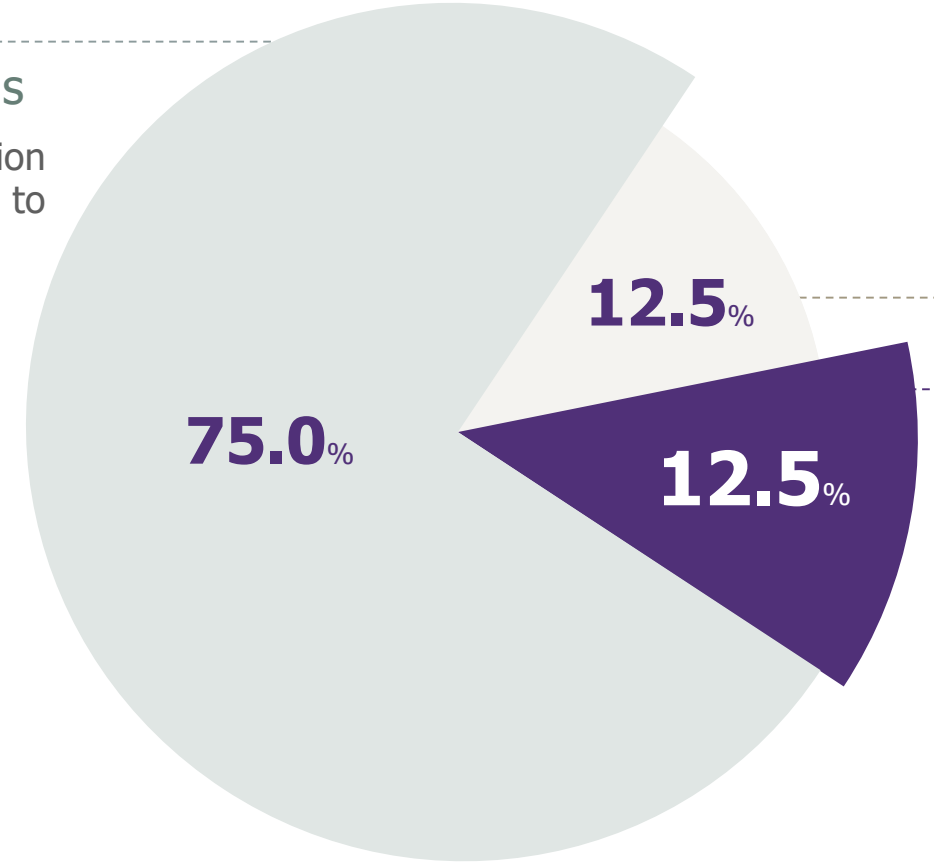
Cybersecurity is integrated into company strategy.



Fragmented investments and at uneven levels

Standalone action plans

There are mentions of action plans implemented in order to deploy security measures.



No mention

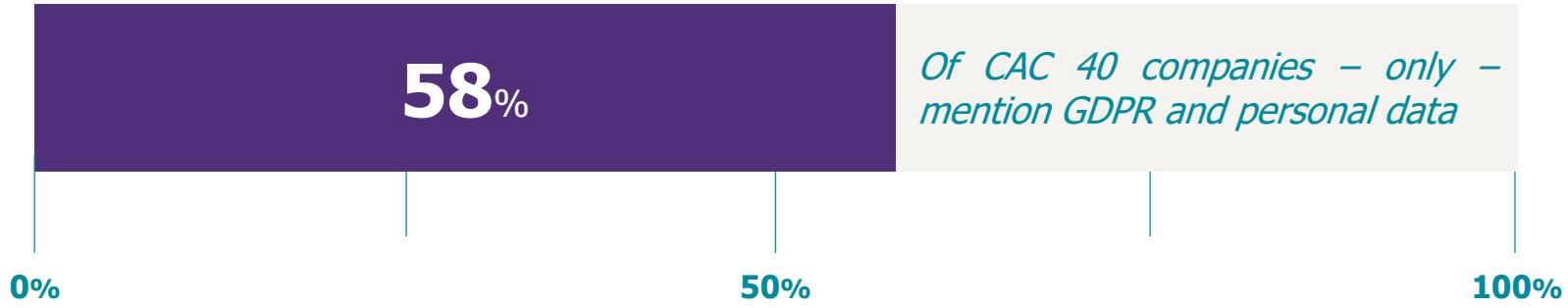
The reports contain no mention of investments aimed to address cybersecurity risks.

Cybersecurity programmes

Security programmes involving significant investments are mentioned.

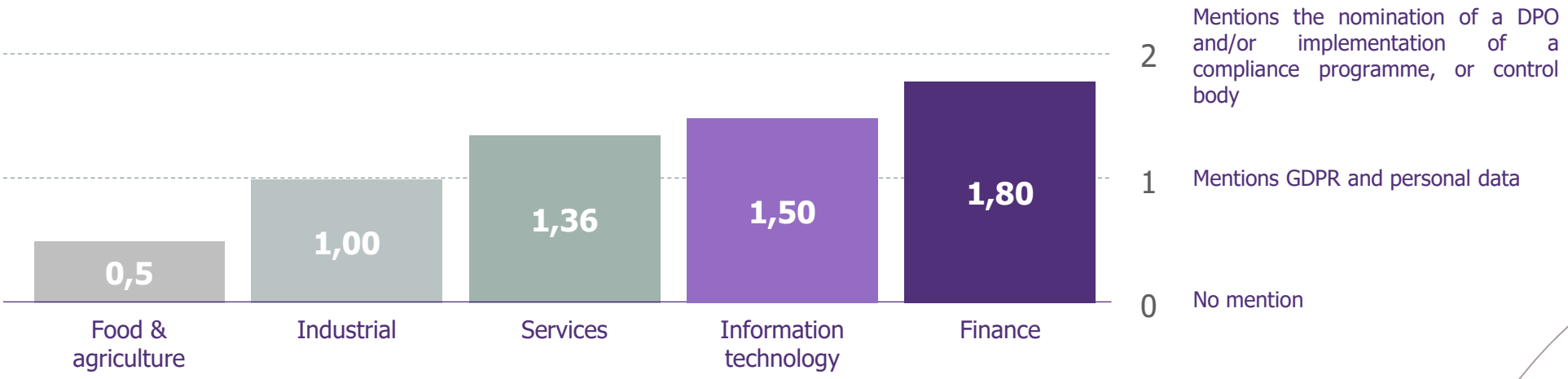
None of the CAC 40 groups mentioned the amount invested but Wavestone has observed cybersecurity programmes on the market going from €50M to €900M. The standalone action plans are each in the range of a few €M.

GDPR* and personal data: the most surprising result?



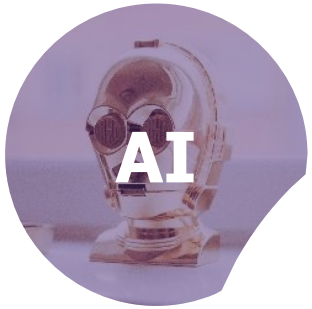
The CAC 40 maturity level has once again been led by the **finance** and **information technology** sectors

.



*GDPR: General Data Protection Regulation

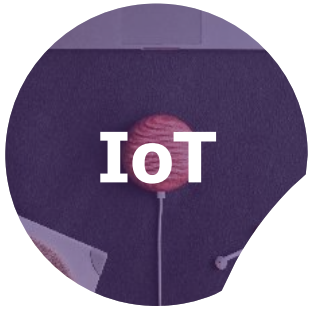
Technological innovations that forget cybersecurity



46% *Of CAC 40 companies mention launching Artificial Intelligence projects*

0% 50% 100%

0 of them link it to cybersecurity



35% *Of CAC 40 companies mention launching Internet of Things projects*

0% 50% 100%

5 – only – link it to cybersecurity

28% *Of CAC 40 companies mention launching blockchain-related projects*

0% 50% 100%

0 of them link it to cybersecurity

Highlights observed in the reports

AWARENESS GOES OUTSIDE THE WALLS OF THE COMPANY

In complement to the usual cybersecurity contractual clauses, a few pioneers have launched awareness and training initiatives for their suppliers, partners or subcontractors.

These practices are to be encouraged as they amplify awareness for the whole economic chain, particularly small and mid cap companies that supply major groups.

BUSINESS RISKS INTEGRATE CYBERSECURITY

The digitalisation of the economy reflects in cyber risks with specific business risks that are mentioned more and more often:

- Industry 4.0;
- Autonomous cars;
- IoT and privacy;
- Fraud in financial services;
- Audio-visual content piracy.

ISO 27001: THE ONLY CYBERSECURITY CERTIFICATION FOR COMPANIES

4 members of the CAC 40 are certified on certain perimeters and 5 base themselves on these international cybersecurity standards.

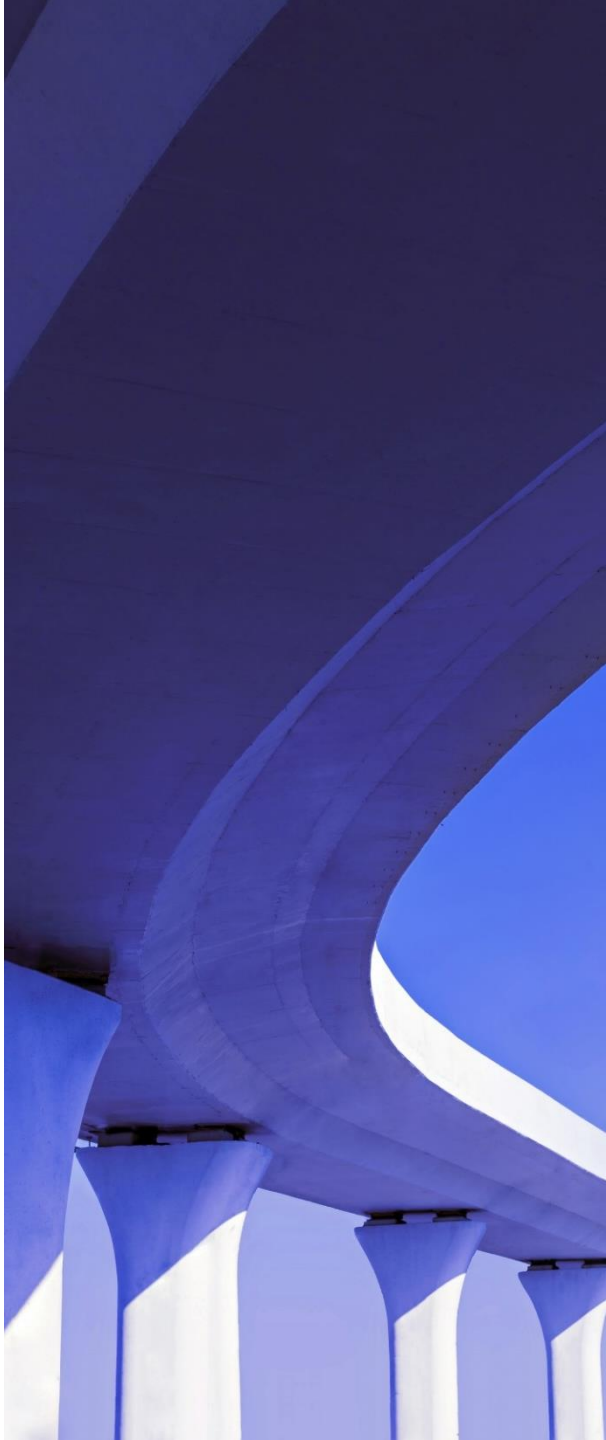
NB: mentions of ANSSI (French cybersecurity agency) and NIST (US standards institute) frameworks appear, providing concrete security measures.

And to conclude

Cybersecurity is taken much more into account in reference documents since 2013…

… but it could be better if the companies put a greater value on the whole of their actions.

For the coming year, an increased transparency on security incidents is expected following the application of GDPR.



APPENDIX

Assessment chart (1/2)

	Weighting	Level 0	Level 1	Level 2
Information security issues and understanding of contextualised threat for the company	3	0 points No mention	+1 point Simple mention of the issues	+2 points Detailed mention of the issues including mentions of how the threat and/or information security specific risks have developed for the business
Cyber risks and its specific impacts on the company's business taken into account	3	0 points No mention	+1 point Mention of cyber risk	+2 points Detailed mention of risk and its impacts
Information security training and awareness	2	0 points No mention	+1 point Mention of awareness for staff and/or ExCo	+2 points Mention of large scale awareness or training initiatives and/or aimed at subcontractors or other external parties
Level of Executive Committee involvement in cybersecurity matters	2	0 points No mention	+1 point Mention of ExCo's involvement	+2 points Mentions the existence of an ExCo member directly involved and responsible for information security topics based on risk control (top owner of IS risk)
Cyber risk handling and coverage: cybersecurity programme and action plan	2	0 points No mention	+1 point Mention of action plans	+2 points Mention of significant investments via a programme (i.e. 10s of M€ or a rough estimate by Wavestone if not specified)
Integrating cybersecurity into digital transformation (AI, Machine Learning, IoT, Blockchain)	1	0 points No mention	+1 point Simple mention	+2 points Detailed mention of the specific risks of new technologies and/or specific securing actions
Information Systems Security (SSI) Governance	2	0 points No mention	+1 point Simple mention of the issues	+2 points Mention of the CISO's hierarchical position and how the organisation is set up at group level

Assessment chart (2/2)

	Weighting	Level 0	Level 1	Level 2
Security of business-specific systems (Industrial control systems, anti-fraud mechanisms, payment systems, etc.)	1	0 points No mention	+1 point Mention of business-specific risks	+2 points Mention of a significant programme and investments
Privacy: GDPR, Privacy, personal data protection	2	0 points No mention	+1 point Simple mention	+2 points Mentions nomination of a DPO and/or implementation of a compliance programme, a control body
Transparency and reaction to publicly announced cyber attacks or major incidents	0	-2 points No mention of a well known incident	-1 point Mention of an incident without its remediation actions	0 point Mention of incidents accompanied by action plans and/or changes made in remediation.
Taking out a cyber insurance policy	0	0 points No mention	+1 point Mentions taking out cyber insurance	+2 points Mention of a level of cyber insurance cover above €100M
Compliance with cybersecurity regulations (NIS, PCI-DSS, French LPM, HADS, NYDFS, etc.)	1	0 points No mention	+1 point Mentions regulations	+2 points Mentions plans to comply with the stated regulations
Respect of cybersecurity standards and certifications (ISO27001, NIST, FFIEC, CIS20, SANS, etc.)	1	0 points No mention	+1 point Mention IS standards	+2 points Mentions compliance, certification or alignment to the stated standards
Information security audit risk control	2	0 points No mention	+1 point Mention of audit and cyber risk coverage measures	+2 points Mentions a specific significant or broad control plan led by the cybersecurity team / internal audit / inspectorate general

WAVESTONE

Gérôme BILLOIS
Partner

M +33 (0)6 10 99 00 60
gerome.billois@wavestone.com

Alexandre LUKAT
Senior Consultant

M +33 (0)6 72 58 26 52
alexandre.lukat@wavestone.com

Dominique YANG
Consultant

M +33 (0)7 62 36 62 28
dominique.yang@wavestone.com

riskinsight-wavestone.com
@Risk_Insight

securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_

PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILANO *

BRUSSELS

GENEVA

CASABLANCA

ISTANBUL *

LYON

MARSEILLE

NANTES

* Partners

WAVESTONE